Divisibilidade e Números primos

George Darmiton da Cunha Cavalcanti
CIn - UFPE

Divisibilidade de inteiros

Sejam ***a*** e ***b*** dois inteiros.

Dizemos que ***a divide b***, ***a é um divisor de b*** ou ***b é um múltiplo de a*** se existe um inteiro ***m*** tal que ***b=am***.

Na notação: a|b.

Se $a \nmid b$, e $a>0$, então é possível dividir ***b*** por ***a*** com resto.

O resto da divisão é um inteiro que satisfaz $0 \leq r < a$.

Se o quociente da divisão com resto é ***q***, então

$$b = aq + r$$

Exemplos

O que significa para a, se (a) $2|a$; (b) $2 \nmid a$; (c) $0|a$.

Prove que

(a) se $a|b$ e $b|c$ então $a|c$;

(b) se $a|b$ e $a|c$ então $a|b+c$ e $a|b-c$;

Números Primos

Um inteiro ***p>1*** é chamado um ***número primo*** se ele não é divisível por qualquer inteiro diferente de ***1***, ***-1***, ***p*** e ***-p***.

Uma outra maneira de dizer isso é que um inteiro ***p>1*** é um primo se ele não pode ser escrito como o produto de dois inteiros positivos menores que ele.

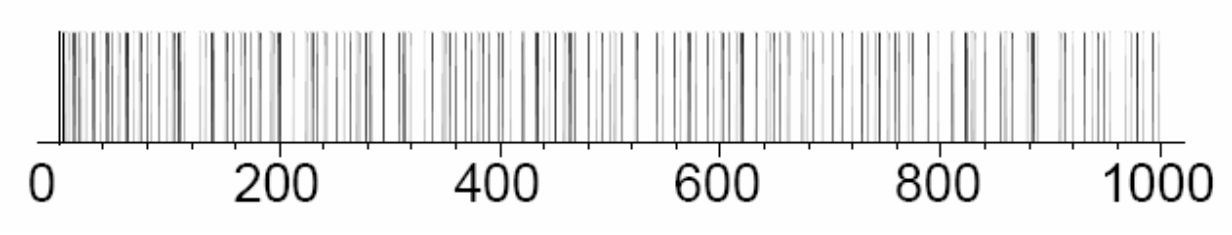
Números Primos

Um inteiro ***n>1*** que não é um primo é chamado ***composto*** (o número 1 não é considerado nem primo, nem composto).

Por conseguinte, 2, 3, 5, 7 e 11 são primos, mas $4=2\times2$, $6=2\times3$, $8=2\times4$, $9=3\times3$ e $10=2\times5$ não são primos.

1, ***2***, ***3***, 4, ***5***, 6, ***7***, 8, 9, 10, ***11***, 12, ***13***, 14, 15, 16, ***17***, 18, ***19***, 20, 21, 22, ***23***, 24, 25, 26, 27, 28, ***29***, 30, ***31***, 32, 33, 34, 35, 36, ***37***, 38, 39, 40, ***41***, 42, ***43***, 44, 45, 46, ***47***, 48, 49, 50, 51, 52, ***53***, 54, 55, 56, 57, 58, ***59***, 60, ***61***, 62, 63, 64, 65, 66, ***67***, 68, 69, 70, ***71***, 72, ***73***, 74, 75, 76, 77, 78, ***79***, 80, 81, 82, ***83***, 84, 85, 86, 87, 88, ***89***, 90, 91, 92, 93, 94, 95, 96, ***97***, 98, 99, 100, ***101***, 102, ***103***, 104, 105, 106, ***107***, 108, ***109***, 110, 111, 112, ***113***, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, ***127***, 128, 129, 130, ***131***, 132, 133, 134, 135, 136, ***137***, 138, ***139***, 140, 141, 142, 143, 144, 145, 146, 147, 148, ***149***, 150, ***151***, 152, 153, 154, 155, 156, ***157***, 158, 159, 160, 161, 162, ***163***, 164, 165, 166, 167, 168, 169, 170, 171, 172, ***173***, 174, 175, 176, 177, 178, ***179***, 180, ***181***, 182, 183, 184, 185, 186, 187, 188, 189, 190, ***191***, 192, ***193***, 194, 195, 196, ***197***, 198, ***199***, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, ***211***, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, ***223***, 224, 225, 226, ***227***, 228, ***229***, 230, 231, 232, 233, 234, 235, 236, 237, 238, ***239***, 240, ***241***, 242, 243, 244, 245, 246, 247, 248, 249, 250, ***251***, 252, 253, 254, 255, 256, ***257***, 258, 259, 260, 261, 262, ***263***, 264, 265, 266, 267, 268, ***269***, 270, ***271***, 272, 273, 274, 275, 276, ***277***, 278, 279, 280, ***281***, 282, ***283***, 284, 285, 286, 287, 288, 289, 290, 291, 292, ***293***, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, ***307***, 308, 309, 310, ***311***, 312, ***313***, 314, 315, 316, ***317***, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, ***331***, 332, 333, 334, 335, 336, ***337***, 338, 339, 340, 341, 342, 343, 344, 345, 346, ***347***, 348, ***349***, 350, 351, 352, ***353***, 354, 355, 356, 357, 358, ***359***, 360, 361, 362, 363, 364, 365, 366, ***367***, 368, 369, 370, 371, 372, ***373***, 374, 375, 376, 377, 378, ***379***, 380, 381, 382, ***383***, 384, 385, 386, 387, 388, ***389***, 390, 391, 392, 393, 394, 395, 396, ***397***, 398, 399, 400, ***401***, 402, 403, 404, 405, 406, 407, 408, ***409***, 410, 411, 412, 413, 414, 415, 416, 417, 418, ***419***, 420, ***421***, 422, 423, 424, 425, 426, 427, 428, 429, 430, ***431***, 432, ***433***, 434, 435, 436, 437, 438, ***439***, 440, 441, 442, ***443***, 444, 445, 446, 447, 448, ***449***, 450, 451, 452, 453, 454, 455, 456, ***457***, 458, 459, 460, ***461***, 462, ***463***, 464, 465, 466, ***467***, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, ***479***, 480, 481, 482, 483, 484, 485, 486, ***487***, 488, 489, 490, ***491***, 492, 493, 494, 495, 496, 497, 498, ***499***, 500

Código de barras dos primos até 1000



Por que estamos interessados nos número primos?

Como será visto no próximo teorema, os primos são, em um sentido multiplicativo, as peças fundamentais dos inteiros.

Fatoração em Primos

Teorema *Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.*

Esse teorema é conhecido também como o "Teorema Fundamental da Teoria dos Números".

Fatoração em Primos

- Por exemplo,
  - Se p é primo, então $p|60$, pois
  - $60 = 6 \times 10$
  - $p|6$ (p=2 ou 3) ou $p|10$ (p=2 ou 5)
  - Assim, $p = 2, 3$ ou 5

Como encontrar a fatoração de um número

$6 = 2 \times 3$

$3 = 3$

$24 = 2 \times 2 \times 2 \times 3$ $(= 2 \times 2 \times 3 \times 2 = 2 \times 3 \times 2 \times 2 = 3 \times 2 \times 2 \times 2)$

A unicidade do teorema pode ser expressa mais precisamente através do uso de expoentes na forma:

$$n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_k^{r_k}$$

sabendo que $p_1 < p_2 < \cdots < p_k$

Prova por contradição

Teorema *O número* $\sqrt{2}$ *é irracional*

Prova

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $n^{1/2}$.

Desse teorema é possível extrair a seguinte informação:

um inteiro é primo se ele não é divisível por nenhum primo menor ou igual a sua raiz quadrada

Exemplo

Mostre que 101 é primo.

Os únicos primos que são menores ou iguais a $101^{½}$ são: 2, 3, 5 e 7.

E como 101 não é divisível por 2, 3, 5, ou 7, pode-se afirmar que 101 é primo.

Infinitude dos Números Primos

Existem duas possibilidades:

- Existe um número finito de primos
- Existe um número infinito de primos

Assumindo que existe um número finito, k.

Os k primos são $p_1,p_2,p_3,...,p_k$ e $n= p_1 \times p_2 \times p_3 \times ... \times p_k + 1$

n é divisível por um dos primos, p_i e

pela definição de divisibilidade $p_1 \times p_2 \times p_3 \times ... \times p_k$ é também divisível por p_i

Assim,

$p_i | (p_1 \times p_2 \times p_3 \times ... \times p_k + 1)$ e $p_i | (p_1 \times p_2 \times p_3 \times ... \times p_k)$, então $p_i | 1$.

O que não é possível, assim nossa hipótese leva a uma contradição.

The Sieve of Eratosthenes

É possível encontrar os primos menores do que um número pré-determinado.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~
19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~ 31 ~~32~~ 33 ~~34~~ 35
~~36~~ 37 ~~38~~ 39 ~~40~~ 41 ~~42~~ 43 ~~44~~ 45 ~~46~~ 47 ~~48~~ 49 ~~50~~

Máximo Divisor Comum

- Como decidir se um dado número é ou não um primo?
- Como encontrar a fatoração prima de um número?
- A chave para uma teoria dos números algorítmica mais avançada é um algoritmo que computa o *máximo divisor comum* de dois inteiros positivos *a* e *b*.
  - Isso é definido como o maior inteiro positivo que é um divisor de ambos.

Máximo Divisor Comum

O máximo divisor comum de ***a*** e ***b*** é representado por ***mdc(a,b)***.

$$\mathrm{mdc}(1,6) = 1, \qquad \mathrm{mdc}(2,6) = 2, \qquad \mathrm{mdc}(3,6) = 3,$$

$$\mathrm{mdc}(4,6) = 2, \qquad \mathrm{mdc}(5,6) = 1, \qquad \mathrm{mdc}(6,6) = 6.$$

Diz-se que dois inteiros são *primos entre si* se seu máximo divisor comum for 1.

É conveniente também definir que $mdc(a,0)=a$, para todo $a \geq 0$.

Mínimo Múltiplo Comum

É o menor inteiro positivo que é um múltiplo de ambos os inteiros, e representado por ***mmc(a,b)***

$$\text{mmc}(1,6) = 6, \qquad \text{mmc}(2,6) = 6, \qquad \text{mmc}(3,6) = 6,$$

$$\text{mmc}(4,6) = 12, \qquad \text{mmc}(5,6) = 30, \qquad \text{mmc}(6,6) = 6$$

Máximo Divisor Comum

O máximo divisor comum de dois inteiros positivos pode ser encontrado um tanto facilmente usando-se as suas fatorações primas.

- Observa-se os fatores primos comuns,eleve-os à menor dos dois expoentes, e toma o produto dessas potências

O problema com esse método é que é muito difícil encontrar a fatoração prima de grandes inteiros.

$300 = 2^2 \times 3 \times 5^2$

$18 = 2 \times 3^2$

Portanto o mdc(300,18) = 2×3 = 6

O algoritmo Euclidiano

Suponha que nos são dados dois inteiros positivos ***a*** e ***b***, e desejamos achar seu máximo divisor comum.

Os seguintes passos devem ser realizados:

1. Se $a > b$ então trocamos a por b e vice-versa.

2. Se $a > 0$, dividimos b por a, para obter um resto r. Substituimos b por r e retornamos ao passo 1.

3. Senão (se $a = 0$), retornamos b como o m.d.c. e paramos.

O algoritmo Euclidiano

$$\mathrm{mdc}(300, 18) = \mathrm{mdc}(12, 18) = \mathrm{mdc}(12, 6) = 6.$$

$$\mathrm{mdc}(101, 100) = \mathrm{mdc}(1, 100) = 1.$$

$$\begin{aligned}\mathrm{mdc}(89, 55) = \mathrm{mdc}(34, 55) &= \mathrm{mdc}(34, 21) = \\ \mathrm{mdc}(13, 21) &= \mathrm{mdc}(13, 8) = \\ \mathrm{mdc}(5, 8) &= \mathrm{mdc}(5, 3) = \\ \mathrm{mdc}(2, 3) &= \mathrm{mdc}(2, 1) = 1.\end{aligned}$$

O algoritmo Euclidiano

Lema

Seja $a=bq+r$,

sabendo que a, b, q e r são inteiros.

Então $mdc(a,b) = mdc(b,r)$.